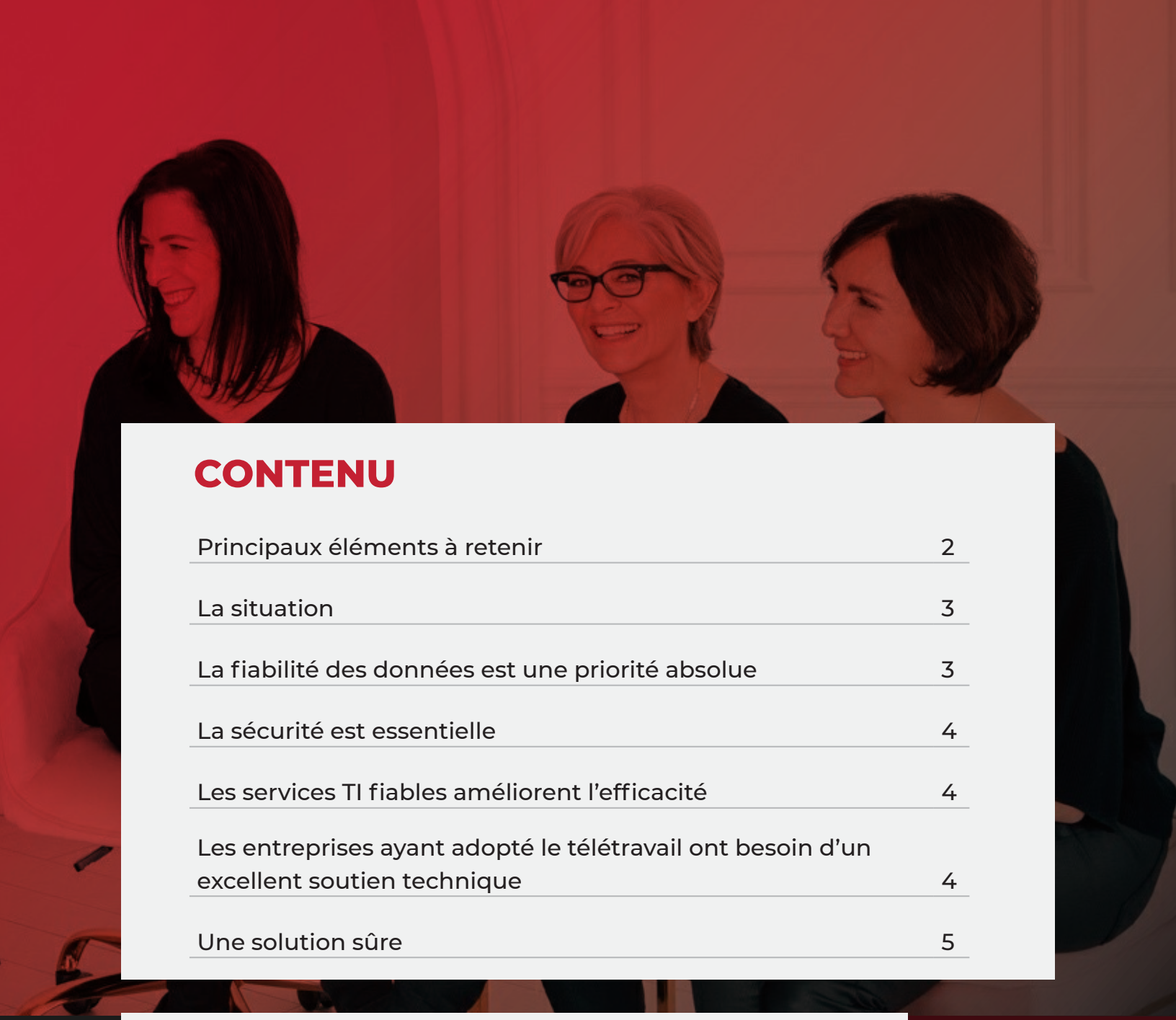
TECHNOLOGIE EN TANT QUE SERVICE POUR LES PETITES ENTREPRISES

ÉTUDE DE CAS

Rand Market Research Corp.
Investir pour protéger les données des clients, améliorer la performance

NPC™
Smarter Computing™



CONTENU

APERÇU

Pour Lee Rand, présidente et fondatrice de Rand Market Research Corp (RMR), la protection des données de son entreprise et de ses clients est une priorité absolue. Elle avait donc besoin d'une technologie informatique de pointe, d'un soutien TI compétent et d'une sécurité évoluée. Le tout en limitant les coûts opérationnels. La solution? Un nouveau modèle de prestation de services de TI : la technologie en tant que service.

DE GAUCHE À DROITE

Amelia Cheston, *gestionnaire de recherche*
Michele Hirak Fletcher, *directrice générale, Stratégie et renseignements*
Eva Blaff, *directrice, Assurance qualité et recrutement*
Lee Rand, *fondatrice et présidente*
Tamara Amar, *directrice, Recherche qualitative*

PRINCIPAUX POINTS À RETENIR

Grâce à la transition vers la technologie en tant que service, RMR profite des performances informatiques, de la sécurité des données et du soutien quotidien de pointe dont son équipe avait besoin. Le tout sans avoir de service informatique dédié ni de nouvelle solution sur mesure créée par un fournisseur local. Cela permet non seulement de réaliser des économies de coûts informatiques, mais aussi de bénéficier d'un service conçu pour les professionnels :

- Un gestionnaire de compte dédié pour tous les besoins informatiques de RMR, ce qui garantit la simplicité et la clarté dans l'achat et le déploiement de la technologie.
- Un soutien technique fiable et compétent qui permet à l'équipe de contacter directement les conseillers techniques pour résoudre tout problème informatique, pour une résolution rapide.
- L'assurance que toutes les données de l'entreprise sont automatiquement sauvegardées en plusieurs versions dans des centres de données sécurisés. Les fichiers perdus et des systèmes entiers peuvent être facilement restaurés.
- Plus de fonctionnalités de collaboration et moins de casse-têtes technologiques : chaque membre de l'équipe utilise les mêmes systèmes et logiciels sur des appareils rapides et hautement sécurisés.
- Les appareils et les données sont chiffrés automatiquement, ce qui réduit les primes d'assurance, et permet aux clients de se vanter d'avoir une protection des données de haut niveau et de passer des questionnaires de sécurité haut la main.
- La technologie en tant que service adoptée par Lee a été mise à l'essai pendant plus d'une décennie avec des milliers de professionnels, et offre des performances informatiques et une sécurité de calibre bancaire à un tarif mensuel abordable, même pour les plus petits bureaux.

LA SITUATION

Fondée par Lee Rand en 1997, Rand Market Research est une agence d'études de marché spécialisée offrant des services de stratégie de marketing et d'information sur les consommateurs à des clients de premier plan d'un large éventail d'industries au Canada et aux États-Unis. Regroupant des spécialistes du marketing et des professionnels de la recherche chevronnés, RMR a bâti des relations durables et à long terme. Elle est reconnue pour son approche axée sur le client et ses solutions aux défis d'affaires et de marketing. La confiance et la qualité des résultats sont au cœur de sa stratégie d'acquisition et de rétention de la clientèle.

Pour que la structure de l'entreprise demeure légère, et l'équipe administrative petite, RMR a externalisé ses besoins en matière de TI et de cybersécurité. Après plusieurs années de services informatiques décevants et de craintes en matière de sécurité, Lee devait trouver un meilleur moyen d'assurer la fiabilité des TI et la cybersécurité de son entreprise.

RMR peut passer des jours, voire des semaines, à travailler sur des documents importants. Ainsi, la perte d'un document ou même d'une version antérieure obligerait l'équipe à revenir à la case départ. Lee croyait que toutes ses données étaient sauvegardées et qu'elle pouvait récupérer un fichier datant de quelques jours, mais elle a plutôt découvert que l'un de ses besoins informatiques les plus fondamentaux n'était pas pleinement satisfait. Cela lui a fait comprendre qu'un système sur mesure – qui n'a pas été testé par des milliers d'utilisateurs dans des centaines d'entreprises – pouvait la rendre vulnérable sans même qu'elle s'en rende compte.

LA FIABILITÉ DES DONNÉES EST UNE PRIORITÉ ABSOLUE

Comme elle travaille avec des clients de haut calibre, dont bon nombre figurent sur la liste Fortune 500, il est primordial pour RMR que les problèmes techniques ne nuisent pas aux opérations commerciales ni, surtout, à la protection des données confidentielles des clients. En fait, la majorité des clients exigent que RMR respecte une norme élevée de protection des données. Aujourd'hui, avec l'importance du télétravail, les entreprises doivent disposer d'un soutien TI rapide et efficace. En effet, même les petits pépins technologiques peuvent avoir des répercussions importantes s'ils empêchent l'équipe de partager les ressources aussi facilement que dans un bureau. En tant qu'entreprise opérant entièrement à distance, RMR a besoin d'outils qui fonctionnent et, en cas de problème, d'un soutien informatique rapide et fiable pour réduire au minimum les temps d'arrêt.

> *Ils avaient commis une erreur – peut-être que mon poste n'avait pas été pris en charge pendant une migration Je ne sais pas ce qui s'est passé, mais je n'avais plus de soutien. C'était extrêmement désagréable. Je me sentais très vulnérable.*
>
> **Lee Rand**
> ***Présidente et fondatrice***
> ***Rand Market Research Corp***

LA SÉCURITÉ EST ESSENTIELLE

Rand Market Research Corp n'a jamais subi de violation de données, mais cette alerte de sécurité a obligé Lee à envisager différentes options.

Tous les professionnels font face à une immense pression en matière de protection des données des clients. Le pire scénario pour un propriétaire d'entreprise est de devoir informer un client qu'un ordinateur portable contenant des données confidentielles a été perdu, ou que leur propriété intellectuelle ou leur travail a été la cible d'une cyberattaque.

Surtout s'il n'est pas en mesure d'indiquer les mesures prises au préalable pour réduire le risque. Informer ses clients d'une telle perte peut être l'expérience la plus stressante qui soit sur le plan professionnel – sans parler des répercussions financières. La mise en place de bonnes pratiques de cybersécurité réduit le risque de violation de données. Lee devait trouver une organisation ou une méthode d'acquisition de services de TI qui respecte de telles pratiques par défaut.

DES SERVICES TI FIABLES AMÉLIORENT L'EFFICACITÉ

Un ordinateur qui ne fonctionne pas correctement en raison d'une défaillance matérielle ou logicielle ou d'une mauvaise configuration nuit non seulement à la sécurité des données, mais aussi à la productivité quotidienne en freinant l'accomplissement des tâches et la réalisation des projets. RMR a souvent dû tenter de résoudre à l'interne des problèmes techniques parce que sa ligne de soutien TI n'était pas toujours utile. En effet, le soutien pouvait prendre plusieurs heures et nécessiter de nombreux appels. En outre, la personne au bout du fil ne possédait pas toujours les connaissances, l'expérience ou les outils nécessaires pour assurer une résolution efficace. Cela représente beaucoup de temps perdu qui aurait pu être consacré à un travail important.

LES ENTREPRISES AYANT ADOPTÉ LE TÉLÉTRAVAIL ONT BESOIN D'UN SOUTIEN TECHNIQUE EXCEPTIONNEL

Le soutien technique est particulièrement essentiel pour les entreprises qui ont adopté le télétravail, car les pépins technologiques peuvent facilement perturber le déroulement de la journée lorsque les collègues travaillent à distance. En effet, impossible de se pencher au-dessus du cubicule ou de se rendre au poste des collègues pour voir s'ils ont le même problème, ni de travailler ensemble à trouver une solution. De plus, le Wi-Fi résidentiel peut présenter des lacunes de configuration et de bande passante causant des problèmes de rendement et de fiabilité que l'on croit à tort causés par l'ordinateur. En cette ère de télétravail, il est essentiel de maintenir la productivité des employés à un niveau élevé et de réduire les frustrations technologiques.

UNE SOLUTION SÛRE

Un conseiller en TI ayant de l'expérience en sécurité des données a informé Lee d'un nouveau modèle de prestation de services qui répondrait à ses besoins en matière de rendement technologique, de soutien et de sécurité, et ce, dans un cadre économique prévisible. Ce modèle, c'est ce que le fournisseur de solutions informatiques gérées et sécurisées NPC DataGuard appelle la « technologie en tant que service ».

Traditionnellement, le matériel et les logiciels utilisés pour exploiter une entreprise de façon sûre et productive sont adaptés et configurés sur mesure. Ainsi, chaque élément – l'appareil, le disque dur, la mémoire et le système d'exploitation ou la suite bureautique – a été choisi individuellement avant d'être organisé en système. Or, cette méthode risque de laisser beaucoup de place à une mauvaise interprétation technique et à des lacunes de sécurité, surtout si le fournisseur de TI local ne possède pas une solide expertise en cybersécurité. Les ordinateurs gérés sécurisés de NPC DataGuard sont des appareils de classe affaires qui sont mis en œuvre de façon normalisée. Testés sur le plan du rendement et de la sécurité, ils sont conçus pour offrir une expérience informatique fiable et hautement performante à chaque utilisateur, chaque fois.

Tous les éléments, du système d'exploitation à la suite Microsoft Office et à l'anti-logiciels malveillants pour entreprise en passant par la sécurité des appareils surveillés et gérés, le chiffrement et la sauvegarde sont choisis, mis en œuvre et configurés par des professionnels de la sécurité. Avec un tel niveau de normalisation, les tests de sécurité approfondis, la surveillance, la gestion et le soutien des appareils sont abordables et pratiques, même pour un seul utilisateur qui travaille à son compte.

Les ordinateurs sécurisés de No Panic Computing (MPC) sont prêts à l'emploi. Leurs disques durs sont chiffrés, la sauvegarde complète des données vers un site distant est configurée et exécutée, et un logiciel de sécurité de calibre militaire surveille de manière proactive les plus récentes cybermenaces. De plus, le service à la clientèle est accessible 24 heures sur 24, 7 jours sur 7 et 365 jours par année. Les techniciens connaissent chaque utilisateur et leur autorisation d'utiliser l'appareil. Ils possèdent une connaissance approfondie du soutien et disposent d'outils connectés à l'appareil pour effectuer les diagnostics et les réparations à la vitesse de l'éclair.

Ainsi, le problème de l'investissement coûteux lié à la sécurité de haut niveau des appareils et des systèmes dans un environnement unique ne se pose plus. La normalisation permet à NPC d'atteindre des niveaux de sécurité importants pour chaque utilisateur et de dépasser les exigences de conformité et de réglementation pour un coût impossible à atteindre à l'interne.

Lee avait trouvé sa solution. Elle a communiqué avec NPC et s'est vu attribuer un gestionnaire de compte. Une évaluation a été effectuée pour déterminer ses besoins particuliers et ses choix de modèle, cerner les enjeux et les préoccupations, et établir un plan pour la migration professionnelle de ses données à partir des systèmes et appareils existants. En l'espace de deux semaines, elle travaillait sur les appareils gérés sécurisés de NPC et sur Microsoft 365.

> *On aime vraiment ça! Je dis « nous » parce que si mon équipe n'est pas heureuse, je ne suis pas heureuse. J'ai l'impression que chacun a ce dont il a besoin.*

Lee et son équipe ont testé (bien involontairement) la promesse de NPC d'une protection améliorée. Devant effectuer un transfert de vol extrêmement serré, une collègue a accidentellement oublié son ordinateur portable dans un avion. Elle a appelé NPC immédiatement.

Après avoir confirmé son identité, le Centre de sécurité de NPC a désactivé l'accès à l'ordinateur et confirmé qu'il y avait une sauvegarde complète de l'appareil dans le centre de données, que toutes les technologies de prévention des intrusions étaient en place et que tout était chiffré pour que personne ne puisse déverrouiller l'ordinateur ni en lire les données. Si quelqu'un tentait de déverrouiller l'ordinateur à plusieurs reprises, les données seraient détruites. Ils ont également commencé à préparer un nouvel appareil et à y charger les données et les configurations de la sauvegarde à distance.

> *Je ne saurais vous dire à quel point je me sens mieux protégée avec NPC.*

C'est pratiquement de la magie! Pendant que le processus de remplacement était en cours, la compagnie aérienne a trouvé l'ordinateur et un appel au centre de sécurité de NPC a heureusement suffi pour le déverrouiller et recharger les identifiants de l'utilisateur autorisé. NPC a aussi annulé la préparation du nouvel appareil. Tous ces services étaient inclus sans frais supplémentaires. Cette expérience a conforté Lee dans sa décision de passer aux solutions informatiques gérées et sécurisées de NPC.

NPC ne peut évidemment pas empêcher un appareil d'être volé, mais elle peut s'assurer que le voleur n'obtient rien d'autre que du matériel. NPC peut verrouiller et localiser l'ordinateur, et en effacer tout le contenu à distance pour que les données ne tombent pas entre de mauvaises mains. De plus, le disque dur est protégé par un chiffrement AES de 256 bits, de sorte que les données sont illisibles pour quiconque ne possède pas la clé.

Lee et son équipe sont reconnaissantes de réaliser d'importantes économies comme dans cet exemple, mais heureusement, ce genre de situation est rare.

Une grande partie de la valeur que Lee et son équipe tirent de NPC est la croissance quotidienne de l'efficience. En effet, l'utilisation d'environnements de travail virtuels et de systèmes d'exploitation normalisés facilite grandement la communication et la collaboration au sein de l'équipe. Le rendement de leurs ordinateurs permet de gérer de lourdes charges de travail, y compris des processus de sauvegarde et de sécurité en arrière-plan.

Lee se sent beaucoup plus en confiance depuis que les données sont sauvegardées régulièrement, de façon fiable et sécurisée. Et son équipe peut travailler avec l'assurance qu'elle ne perdra pas un travail important pour elle, mais aussi pour ses clients.

Le fait d'outiller son équipe avec des ordinateurs gérés sécurisés par NPC réduit même les primes d'assurance en raison des mesures proactives prises contre les cybermenaces et les responsabilités légales.

Le soutien technique que RMR reçoit en tout temps de NPC a représenté une nette amélioration.

« En un sens, notre modèle de prestation de services offre tous les avantages, explique Bill Keating, vice-président de la technologie et des opérations de NPC. Bien que chaque appareil soit sécurisé pour chaque utilisateur, notre communauté utilise des appareils normalisés dans une configuration testée que nous avons conçue et construite; nos outils avancés de sécurité, de diagnostic et de soutien sont toujours prêts. Avec ce modèle, vous pouvez vous attendre à une meilleure expérience utilisateur, à moins d'incidents de soutien et à des temps de résolution plus courts. »

> *Le fait de disposer d'un unique numéro que chacun des membres de notre équipe peut utiliser au besoin nous a permis de gagner beaucoup de temps,*
>
> **ajoute Lee.**

Lorsque Lee ou un membre de son équipe appelle pour un problème technique, ils reçoivent l'aide immédiate d'un expert.

Parfois, ils ont besoin d'aide pour configurer une imprimante ou une webcam. D'autres fois, c'est un problème plus complexe qui amène Bill et son équipe technique principale à travailler directement avec les fournisseurs. Quoi qu'il en soit, Lee et son équipe ne sont jamais laissés à elles-mêmes.

« Nous sommes le point de contact unique pour tout ce que nous fournissons à nos clients. Aucun client de NPC n'a jamais eu à appeler un fournisseur de matériel, Microsoft, ni le fournisseur d'antivirus. Avec nous, pas besoin d'analyser les coûts de diagnostic ni de savoir si un appareil est sous garantie. Nous offrons du soutien pour tout ce que nous fournissons, sans frais supplémentaires, et chaque composant est toujours couvert par la garantie, peu importe le fournisseur d'origine, poursuit Bill. Même si un appareil tombe et se brise, ou si on a renversé du café dessus, nous le remplaçons gratuitement et restaurons les données et les applications. »

Il convient également de noter que le taux de résolution des problèmes techniques au premier appel de NPC est supérieur à 85 % et que le temps moyen pour communiquer avec un représentant est inférieur à 90 secondes.

Lee en est à sa deuxième série d'appareils et de services avec NPC, car l'ensemble des ordinateurs sont remplacés tous les trois ans par les plus récents modèles de classe affaires.

Le mot de la fin revient à notre précieuse cliente, Lee :

> *NPC a été un gros avantage pour nous et je me félicite de les avoir choisis. Lorsque je pense à l'extraordinaire augmentation des cyberattaques ces dernières années que l'on voit dans les médias, il est rassurant de savoir que j'ai investi dans l'informatique sécurisée et que NPC est toujours au travail pour protéger mon entreprise et mes clients.*

Appelez-nous ou écrivez-nous dès aujourd'hui!

Pour une consultation gratuite sur la façon dont la technologie en tant que service peut réduire vos coûts et augmenter votre sécurité et votre rendement.

:1 855 667-2642 :info@npcdataguard.com